

1. What is a characteristic of a fault tolerant network?

- a network that protects confidential information from unauthorized access
- a network that can expand quickly to support new users and applications without impacting the performance of the service delivered to existing users
- a network that supports a mechanism for managing congestion and ensuring reliable delivery of content to all users
- a network that recovers quickly when a failure occurs and depends on redundancy to limit the impact of a failure

Explanation:

Fault tolerant networks limit the impact of a failure because the networks are built in a way that allows for recovery when a failure occurs. These networks depend on multiple or redundant paths between the source and destination of a message. A scalable network can expand quickly to support new users and applications without impacting the performance of the service delivered to existing users.

Quality of service (QoS) is a mechanism for managing congestion and ensuring reliable delivery of content.

2. Three bank employees are using the corporate network. The first employee uses a web browser to view a company web page in order to read some announcements. The second employee accesses the corporate database to perform some financial transactions. The third employee participates in an important live audio conference with other corporate managers in branch offices. If QoS is implemented on this network, what will be the priorities from highest to lowest of the different data types?

- audio conference, financial transactions, web page
- financial transactions, web page, audio conference
- audio conference, web page, financial transactions
- financial transactions, audio conference, web page

Explanation:

QoS mechanisms enable the establishment of queue management strategies that enforce priorities for different types of data. Thus, this queuing enables voice data to have priority over transaction data, which has priority over web data.

3. What is a benefit of using cloud computing in networking?

- End users have the freedom to use personal tools to access information and communicate across a business network.
- Network capabilities are extended without requiring investment in new infrastructure, personnel, or software.
- Technology is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated.
- Home networking uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

Explanation:

Cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or developing new software. These services are available on-demand and delivered economically to any device anywhere in the world. BYOD is about end users having the freedom to use personal tools to access information.

business or campus network. Smart home technology is integrated into every-day appliances allowing the making them more 'smart' or automated. Powerline networking is a trend for home networking that uses devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

4. What is the function of the shell in an OS?

- It interacts with the device hardware.
- **It interfaces between the users and the kernel.**
- It provides dedicated firewall services.
- It provides the intrusion protection services for the device.

Explanation:

Most operating systems contain a shell and a kernel. The kernel interacts with the hardware and the shell users.

5. Which connection provides a secure CLI session with encryption to a Cisco switch?

- a console connection
- an AUX connection
- a Telnet connection
- **an SSH connection**

Explanation:

A CLI session using Secure Shell (SSH) provides enhanced security because SSH supports strong password transport of session data. The other methods support authentication but not encryption.

6. A network technician is attempting to configure an interface by entering the following command: SanJose(config)# ip address 192.168.2.1 255.255.255.0. The command is rejected by the device. What is the reason for this?

- **The command is being entered from the wrong mode of operation.**
- The command syntax is wrong.
- The subnet mask information is incorrect.
- The interface is shutdown and must be enabled before the switch will accept the IP address.

Explanation:

The wrong mode of operation is being used. The CLI prompt indicates that the mode of operation is global configuration mode. The command should be configured from interface configuration mode, as indicated by the SanJose(config-if)# prompt.

7. An administrator uses the Ctrl-Shift-6 key combination on a switch after issuing the ping command. What is the purpose of using these keystrokes?

- to restart the ping process
- **to interrupt the ping process**
- to exit to a different configuration mode
- to allow the user to complete the command

Explanation:

To interrupt an IOS process such as **ping** or **traceroute**, a user enters the Ctrl-Shift-6 key combination. To exit from configuration mode to privileged mode use the **end** command. To reissue the **ping** command, the user must first reenter the **ping** command, thus making it easier for the user to press Enter and reissue the **ping** command.

8. Refer to the exhibit. A network administrator is configuring access control to switch SW1. If the administrator uses a console connection to connect to the switch, which password is needed to access user EXEC mode?

```
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# enable password letmein
SW1(config)# enable secret secretin
SW1(config)# line console 0
SW1(config-line)# password lineconin
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# line vty 0 15
SW1(config-line)# password linevtyin
SW1(config-line)# login
SW1(config-line)# end
SW1#
```

ITN Final Exam Form A Answers 002

- letmein
- secretin
- **lineconin**
- linevtyin

Explanation:

Telnet accesses a network device through the virtual interface configured with the **line VTY** command. The password configured under the **line console 0** command is required to access the user EXEC mode. The password configured under the **line console 0** command is for the console port, and the enable and enable secret passwords are used to allow entry into the privileged EXEC mode.

9. On which switch interface would an administrator configure an IP address so that the switch can be managed remotely?

- FastEthernet0/1
- **VLAN 1**
- vty 0
- console 0

Explanation:

Interface VLAN 1 is a virtual interface on a switch, called SVI (switch virtual interface). Configuring an IP address on interface VLAN 1, will allow a switch to be accessed remotely. The VTY line must also be configured to allow access. The IP address cannot be configured on this line.

10. What protocol is responsible for controlling the size of segments and the rate at which segments are exchanged between a web client and a web server?

- TCP
- IP
- HTTP
- Ethernet

Explanation:

TCP is a Layer 4 protocol of the OSI model. TCP has several responsibilities in the network communication. It breaks data into smaller segments which are more efficient to send across the network. It also controls the size and rate of data sent between clients and servers.

11. What is an advantage to using a protocol that is defined by an open standard?

- A company can monopolize the market.
- The protocol can only be run on equipment from a specific vendor.
- An open standard protocol is not controlled or regulated by standards organizations.
- It encourages competition and promotes choices.

Explanation:

A monopoly by one company is not a good idea from a user point of view. If a protocol can only be run on equipment from a specific vendor, it can have mixed equipment in a network. A proprietary protocol is not free to use. An open standard protocol allows a wide range of vendors.

12. What are two benefits of using a layered network model? (Choose two.)

- It assists in protocol design.
- It speeds up packet delivery.
- It prevents designers from creating their own model.
- It prevents technology in one layer from affecting other layers.
- It ensures a device at one layer can function at the next higher layer.

Explanation:

Some vendors have developed their own reference models and protocols. Today, if a device is to communicate, it must use the TCP/IP model. The benefits of using a layered model are as follows:

- assists in protocol design
- fosters competition between vendors
- prevents a technology that functions at one layer from affecting any other layer
- provides a common language for describing network functionality
- helps in visualizing the interaction between each layer and protocols between each layer

13. Which two OSI model layers have the same functionality as two layers of the TCP/IP model? (Choose two.)

- data link
- network
- physical

- session
- **transport**

Explanation:

The OSI transport layer is functionally equivalent to the TCP/IP transport layer, and the OSI network layer and data link layer together are equivalent to the TCP/IP network access layer. The OSI presentation layer is included within the TCP/IP application layer.

14. Which name is assigned to the transport layer PDU?

- bits
- data
- frame
- packet
- **segment**

Explanation:

Application data is passed down the protocol stack on its way to be transmitted across the network media. As protocols add information to it at each level. At each stage of the process, a PDU (protocol data unit) has functions. The PDUs are named according to the protocols of the TCP/IP suite:

- **Data** – The general term for the PDU used at the application layer.
- **Segment** – transport layer PDU
- **Packet** – network layer PDU
- **Frame** – data link layer PDU
- **Bits** – A physical layer PDU used when physically transmitting data over the medium

15. A network administrator is troubleshooting connectivity issues on a server. Using a tester, the administrator notices that the signals generated by the server NIC are distorted and not usable. In which layer of the OSI model is the error categorized?

- presentation layer
- network layer
- **physical layer**
- data link layer

Explanation:

The NIC has responsibilities in both Layer 1 and Layer 2. The NIC encodes the frame as a series of signals over the media. This is the responsibility of the physical layer of the OSI model. The signal could be in the form of light or radio waves.

16. A network administrator is measuring the transfer of bits across the company backbone for a mission critical financial application. The administrator notices that the network throughput appears lower than the bandwidth expected. Which three factors could influence the differences in throughput? (Choose three.)

- **the amount of traffic that is currently crossing the network**
- the sophistication of the encapsulation method applied to the data
- **the type of traffic that is crossing the network**

- the latency that is created by the number of network devices that the data is crossing
- the bandwidth of the WAN connection to the Internet
- the reliability of the gigabit Ethernet infrastructure of the backbone

Explanation:

Throughput usually does not match the specified bandwidth of physical links due to multiple factors. The traffic, type of traffic, and latency created by the network devices the data has to cross.

17. What is a characteristic of UTP cabling?

- cancellation
- cladding
- immunity to electrical hazards
- woven copper braid or metallic foil

Explanation:

Cladding and immunization from electrical hazards are characteristics for fiber-optic cabling. A woven copper braid or metallic foil acts as a shield for the inner coaxial cable conductor. Cancellation is a property of UTP cabling where two wires are twisted together so each magnetic field cancels out the adjacent magnetic field.

18. What are two characteristics of fiber-optic cable? (Choose two.)

- It is not affected by EMI or RFI.
- Each pair of cables is wrapped in metallic foil.
- It combines the technique of cancellation, shielding, and twisting to protect data.
- It typically contains 4 pairs of fiber-optic wires.
- It is more expensive than UTP cabling is.

Explanation:

Fiber-optic cabling supports higher bandwidth than UTP for longer distances. Fiber is immune to EMI and RFI, requires less skill to install, and requires more safety precautions.

19. What is a characteristic of the LLC sublayer?

- It provides the logical addressing required that identifies the device.
- It provides delimitation of data according to the physical signaling requirements of the medium.
- It places information in the frame allowing multiple Layer 3 protocols to use the same network interface and media.
- It defines software processes that provide services to the physical layer.

Explanation:

The Logical Link Control (LLC) defines the software processes that provide services to the network layer. It identifies which network layer protocol is being used for the frame. This information allows protocols, such as IPv4 and IPv6, to utilize the same network interface and media.

20. A network team is comparing physical WAN topologies for connecting remote sites to a headquarters building. Which topology provides high availability and connects some, but not all, remote sites?

- mesh
- **partial mesh**
- hub and spoke
- point-to-point

Explanation:

Partial mesh topologies provide high availability by interconnecting multiple remote sites, but do not require every site to be connected to every other site. A mesh topology requires point-to-point links with every system being connected to every other system where each device is connected to one other device. A hub and spoke uses a central device in a star topology to connect multiple point devices.

21. What method is used to manage contention-based access on a wireless network?

- CSMA/CD
- priority ordering
- **CSMA/CA**
- token passing

Explanation:

Carrier sense multiple access with collision avoidance (CSMA/CA) is used with wireless networking technology. Carrier sense multiple access with collision detection (CSMA/CD) is used with wired Ethernet technology. Priority ordering and token passing are not used (or not a method) for media access control.

22. What are the three primary functions provided by Layer 2 data encapsulation? (Choose three.)

- error correction through a collision detection method
- session control using port numbers
- **data link layer addressing**
- placement and removal of frames from the media
- **detection of errors through CRC calculations**
- **delimiting groups of bits into frames**
- conversion of bits into data signals

Explanation:

Through the framing process, delimiters are used to identify the start and end of the sequence of bits that are being transmitted. Data link layer addressing is added to enable a frame to be delivered to a destination node. A cyclic redundancy check (CRC) is calculated on the data and added to the frame. If the CRC value contained in the arriving frame is the same as the one the receiver calculated, the frame is accepted and processed.

23. What will a host on an Ethernet network do if it receives a frame with a destination MAC address that does not match its own MAC address?

- **It will discard the frame.**
- It will forward the frame to the next host.
- It will remove the frame from the media.
- It will strip off the data-link frame to check the destination IP address.

Explanation:

In an Ethernet network, each NIC in the network checks every arriving frame to see if the destination MAC address matches its own MAC address. If there is no match, the device discards the frame. If there is a match, the NIC passes the frame to the CPU.

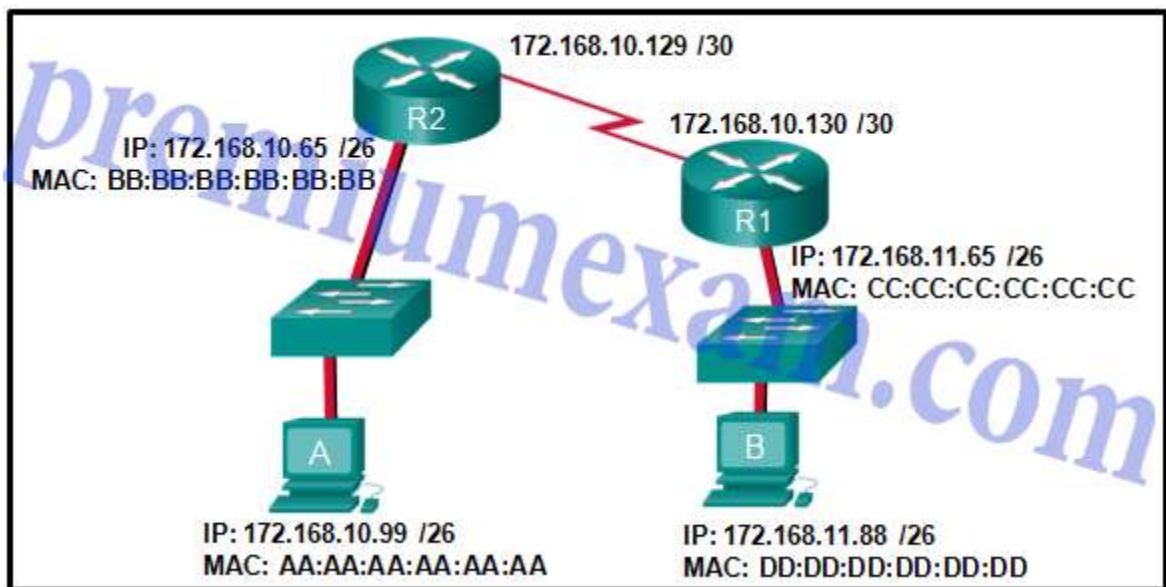
24. Which frame forwarding method receives the entire frame and performs a CRC check to detect errors before forwarding the frame?

- cut-through switching
- **store-and-forward switching**
- fragment-free switching
- fast-forward switching

Explanation:

Fast-forward and fragment-free switching are variations of cut-through switching, which begins to forward a frame as soon as the destination MAC address is received.

25. Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?



ITN Final Exam Form A Answers 001

- DD:DD:DD:DD:DD:DD
- 172.168.10.99
- CC:CC:CC:CC:CC:CC
- 172.168.10.65
- **BB:BB:BB:BB:BB:BB**
- AA:AA:AA:AA:AA:AA

Explanation:

When a host sends information to a distant network, the Layer 2 frame header will contain a source and destination address. The source address will be the originating host device. The destination address will be the router interface that connects the host to the network.

of host A sending information to host B, the source address is AA:AA:AA:AA:AA:AA and the destination assigned to the R2 Ethernet interface, BB:BB:BB:BB:BB:BB.

26. What addresses are mapped by ARP?

- destination MAC address to a destination IPv4 address
- destination IPv4 address to the source MAC address
- destination IPv4 address to the destination host name
- destination MAC address to the source IPv4 address

Explanation:

ARP, or the Address Resolution Protocol, works by mapping a destination MAC address to a destination destination IPv4 address and uses ARP to resolve the corresponding destination MAC address.

27. What are two services provided by the OSI network layer? (Choose two.)

- performing error detection
- routing packets toward the destination
- encapsulating PDUs from the transport layer
- placement of frames on the media
- collision detection

Explanation:

The OSI network layer provides several services to allow communication between devices:

- addressing
- encapsulation
- routing
- de-encapsulation

Error detection, placing frames on the media, and collision detection are all functions of the data link layer.

28. What are two functions of NVRAM? (Choose two.)

- to store the routing table
- to retain contents when power is removed
- to store the startup configuration file
- to contain the running configuration file
- to store the ARP table

Explanation:

NVRAM is permanent memory storage, so the startup configuration file is preserved even if the router loses power.

29. Refer to the exhibit. What will be the result of entering this configuration the next time a network administrator connects a console cable to the router and no additional commands have been entered?

```

R1#config t
R1(config)#enable password Cisco123
R1(config)#enable secret Cisco234
R1(config)#service password-encryption
R1(config)#line con 0
R1(config-line)#password Cisco789
R1(config-line)#end
R1#copy running-config startup-config
R1#reload

```

ITN Final Exam Form A Answers 003

- The administrator will be required to enter Cisco123.
- The administrator will be required to enter Cisco234.
- The administrator will be required to enter Cisco789.
- **The administrator will be presented with the R1> prompt.**

Explanation:

Until both the **password** *password* and the **login** commands are entered in console line configuration mode, access to enable mode.

30. What is the dotted decimal representation of the IPv4 address 11001011.00000000.01110001.11010011?

- 192.0.2.199
- 198.51.100.201
- **203.0.113.211**
- 209.165.201.223

Explanation:

Each section (octet) contains eight binary digits. Each digit represents a specific value (128, 64, 32, 16, 8, 4, 2, 1, the specific value is relevant. Add all relevant values in a particular octet to obtain the decimal value. For the first octet, 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 203 in decimal.

31. What are three characteristics of multicast transmission? (Choose three.)

- The source address of a multicast transmission is in the range of 224.0.0.0 to 224.0.0.255.
- **A single packet can be sent to a group of hosts.**
- **Multicast transmission can be used by routers to exchange routing information.**
- **Routers will not forward multicast addresses in the range of 224.0.0.0 to 224.0.0.255.**
- Computers use multicast transmission to request IPv4 addresses.
- Multicast messages map lower layer addresses to upper layer addresses.

Explanation:

Broadcast messages consist of single packets that are sent to all hosts on a network segment. These types of messages are used by routing protocols, such as OSPF and RIPv2, to exchange routes. The address range 224.0.0.0 to 224.0.0.255 is used by routing protocols to reach multicast groups on a local network.

32. What are the three ranges of IP addresses that are reserved for internal private use? (Choose three.)

- 10.0.0.0/8
- 64.100.0.0/14
- 127.16.0.0/12
- 172.16.0.0/12
- 192.31.7.0/24
- 192.168.0.0/16

Explanation:

The private IP address blocks that are used inside companies are as follows:

- 10.0.0.0 /8 (any address that starts with 10 in the first octet)
- 172.16.0.0 /12 (any address that starts with 172.16 in the first two octets through 172.31.255.255)
- 192.168.0.0 /16 (any address that starts with 192.168 in the first two octets)

33. What purpose does NAT64 serve in IPv6?

- It converts IPv6 packets into IPv4 packets.
- It translates private IPv6 addresses into public IPv6 addresses.
- It enables companies to use IPv6 unique local addresses in the network.
- It converts regular IPv6 addresses into 64-bit addresses that can be used on the Internet.
- It converts the 48-bit MAC address into a 64-bit host address that can be used for automatic host addressing.

Explanation:

NAT64 is typically used in IPv6 when networks are being transitioned from IPv4 to IPv6. It allows the IPv6 networks (such as the Internet), and works by translating the IPv6 packets into IPv4 packets.

34. What is the most compressed representation of the IPv6 address 2001:0000:0000:abcd:0000:0000:0000:0001?

- 2001:0:abcd::1
- 2001:0:0:abcd::1
- 2001::abcd::1
- 2001:0000:abcd::1
- 2001::abcd:0:1

Explanation:

The IPv6 address 2001:0000:0000:abcd:0000:0000:0000:0001 in its most compressed format would be 2001::abcd::1. The four leading zeros would each compress to a single zero. The three consecutive hexets of zeros can be compressed to a double colon ::. The leading zeros in the last hexet can be removed. The double colon :: can only be used once in an address.

35. Which range of link-local addresses can be assigned to an IPv6-enabled interface?

- FEC0::/10
- FDEE::/7
- **FE80::/10**
- FF00::/8

Explanation:

Link-local addresses are in the range of FE80::/10 to FEBF::/10. The original IPv6 specification defined a prefix range FEC0::/10, but these addresses were deprecated by the IETF in favor of unique local addresses because it is in the range of FC00::/7 to FDFF::/7. IPv6 multicast addresses have the prefix FF00::/8.

36. How many valid host addresses are available on an IPv4 subnet that is configured with a /26 mask?

- 254
- 190
- 192
- 62
- 64

Explanation:

When a /26 mask is used, 6 bits are used as host bits. With 6 bits, 64 addresses are possible, but one address is for a broadcast. This leaves 62 addresses that can be assigned to network devices.

37. A site administrator has been told that a particular network at the site must accommodate 126 hosts. Which subnet mask would be used that contains the required number of host bits?

- 255.255.255.0
- 255.255.255.128
- 255.255.255.224
- 255.255.255.240

Explanation:

The subnet mask of 255.255.255.0 has 8 host bits. The mask of 255.255.255.128 results in 7 host bits. The mask of 255.255.255.224 results in 5 host bits. Finally, 255.255.255.240 represents 4 host bits.

38. Which subnet would include the address 192.168.1.96 as a usable host address?

- 192.168.1.64/26
- 192.168.1.32/27
- 192.168.1.32/28
- 192.168.1.64/29

Explanation:

For the subnet of 192.168.1.64/26, there are 6 bits for host addresses, yielding 64 possible addresses. However, the network and broadcast addresses for this subnet are 192.168.1.64 and 192.168.1.127, respectively. Therefore, the range of host addresses for this subnet is 192.168.1.65 to 192.168.1.126. The other subnets do not contain the address 192.168.1.96 as a valid host address.

39. Which statement is true about variable-length subnet masking?

- Each subnet is the same size.
- The size of each subnet may be different, depending on requirements.
- Subnets may only be subnetted one additional time.
- Bits are returned, rather than borrowed, to create additional subnets.

Explanation:

In variable-length subnet masking, bits are borrowed to create subnets. Additional bits may be borrowed from the original subnets. This may continue until there are no bits available to borrow.

40. Which scenario describes a function provided by the transport layer?

- A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address used to contact another network device on the same network.
- A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header.
- A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.
- A corporate worker is accessing a web server located on a corporate network. The transport layer formats the screen so the web page appears properly no matter what device is being used to view the web site.

Explanation:

The source and destination port numbers are used to identify the correct application and window within the

41. A user opens three browsers on the same PC to access www.cisco.com to search for certification course information. The Cisco web server sends a datagram as a reply to the request from one of the web browsers. Which information is used by the TCP/IP protocol stack in the PC to identify which of the three web browsers should receive the reply?

- the destination IP address
- the destination port number
- the source IP address
- the source port number

Explanation:

Each web browser client application opens a randomly generated port number in the range of the registered source port number in the datagram that it sends to a server. The server then uses this port number as the destination port number in the datagram that it sends to the web browser. The PC that is running the web browser application receives the datagram and uses the port number that is contained in this datagram to identify the client application.

42. What are two ways that TCP uses the sequence numbers in a segment? (Choose two.)

- to identify missing segments at the destination
- to reassemble the segments at the remote location
- to specify the order in which the segments travel from source to destination
- to limit the number of segments that can be sent out of an interface at one time
- to determine if the packet changed during transit

43. Which two tasks are functions of the presentation layer? (Choose two.)

- compression
- addressing
- encryption
- session control
- authentication

Explanation:

The presentation layer deals with common data format. Encryption, formatting, and compression are some of the functions of this layer. Addressing occurs in the network layer, session control occurs in the session layer, and authentication takes place in the application layer.

44. What is a key characteristic of the peer-to-peer networking model?

- wireless networking
- social networking without the Internet
- network printing using a print server
- resource sharing without a dedicated server

Explanation:

The peer-to-peer (P2P) networking model allows data, printer, and resource sharing without a dedicated server.

45. A technician can ping the IP address of the web server of a remote company but cannot successfully ping the URL address of the same web server. Which software utility can the technician use to diagnose the problem?

- tracert
- ipconfig
- netstat
- nslookup

Explanation:

Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path from the source to the destination. It can provide important verification and troubleshooting information. The ipconfig utility is used to display the IP configuration of a Windows PC. The Netstat utility is used to identify which active TCP connections are open and running on the system. The nslookup utility allows the user to manually query the name servers to resolve a given host name. This utility is used to diagnose DNS resolution issues and to verify the current status of the name servers.

46. Which domain name would be an example of a top-level domain?

- www.cisco.com
- cisco.com
- .com
- root.cisco.com

Explanation:

Top-level domains represent a country or type of organization, such as .com or .edu.

47. A PC obtains its IP address from a DHCP server. If the PC is taken off the network for repair, what happens to the IP address configuration?

- The configuration is permanent and nothing changes.
- The address lease is automatically renewed until the PC is returned.
- The address is returned to the pool for reuse when the lease expires.
- The configuration is held by the server to be reissued when the PC is returned.

Explanation:

When a DHCP address is issued to a host, it is for a specific lease time. Once the lease expires, the address is returned to the pool for reuse.

48. A wireless host needs to request an IP address. What protocol would be used to process the request?

- FTP
- HTTP
- DHCP
- ICMP
- SNMP

Explanation:

The DHCP protocol is used to request, issue, and manage IP addressing information. CSMA/CD is the access method for Ethernet. ICMP is used to test connectivity. SNMP is used with network management and FTP is used for file transfer.

49. Which example of malicious code would be classified as a Trojan horse?

- malware that was written to look like a video game
- malware that requires manual user intervention to spread between systems
- malware that attaches itself to a legitimate program and spreads to other programs when launched
- malware that can automatically spread from one system to another by exploiting a vulnerability in the target

Explanation:

A Trojan horse is malicious code that has been written specifically to look like a legitimate program. This code simply attaches itself to an actual legitimate program. Viruses require manual intervention from a user to spread, while a worm is able to spread automatically between systems by exploiting vulnerabilities on those devices.

50. When applied to a router, which command would help mitigate brute-force password attacks against the router?

- exec-timeout 30
- service password-encryption
- banner motd \$Max failed logins = 5\$
- login block-for 60 attempts 5 within 60

Explanation:

The **login block-for** command sets a limit on the maximum number of failed login attempts allowed within a specified period of time. If the limit is exceeded, no further logins are allowed for the specified period of time. This helps to mitigate brute-force password attacks. The **exec-timeout** command sets the amount of time a user can be idle before the router disconnects the session.

idle before the user is disconnected. The **service password-encryption** command encrypts the passwords. The **banner motd** command displays a message to users who are logging in to the device.

51. A network technician suspects that a particular network connection between two Cisco switches is having a duplex mismatch. Which command would the technician use to see the Layer 1 and Layer 2 details of a switch port?

- **show interfaces**
- show running-config
- show ip interface brief
- show mac-address-table

Explanation:

The **show interfaces** command can be used on both routers and switches to see speed, duplex, media type, and other Layer 1/Layer 2-related information.

52. Where are Cisco IOS debug output messages sent by default?

- memory buffers
- vty lines
- Syslog server
- **console line**

Explanation:

Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the Syslog server is configured with the **terminal monitor** command.

53. Match the description with the associated IOS mode. (Not all options are used.)

changes made affect the operation of the device as a whole	user EXEC mode
accessed by entering the enable command	✓ limited number of basic monitoring commands
identified by a prompt ending with the # character	✓ the first entrance into the CLI of an IOS device
limited number of basic monitoring commands	privileged EXEC mode
accessed by entering the configure terminal command	✓ accessed by entering the enable command
the first entrance into the CLI of an IOS device	✓ identified by a prompt ending with the # character
used to enable the password for vty lines	global configuration mode
	✓ changes made affect the operation of the device as a whole
	✓ accessed by entering the configure terminal command

ITN Final Exam Form A Answers 01

54. Refer to the exhibit. Match the packets with their destination IP address to the exiting interfaces on the router. (Not all targets are used.)

```

<output omitted>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
  10.0.0.0/24 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, Serial0/0/0
  172.17.0.0/24 is subnetted, 4 subnets
O    172.17.6.0 [110/2] via 192.168.3.4, 00:10:41, FastEthernet0/0
O    172.17.10.0 [110/2] via 192.168.5.2, 00:09:52, FastEthernet1/1
O    172.17.12.0 [110/2] via 192.168.4.2, 00:12:23, FastEthernet1/0
C    172.17.14.0 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
C    192.168.5.0/24 is directly connected, FastEthernet1/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0

```

packets with destination of 172.17.10.5	FastEthernet0/0 ✓ packets with destination of 172.17.6.15
packets with destination of 172.17.12.10	FastEthernet0/1 ✓ packets with destination of 172.17.14.8
packets with destination of 172.17.14.8	FastEthernet1/0 ✓ packets with destination of 172.17.12.10
packets with destination of 172.17.8.20	FastEthernet1/1 ✓ packets with destination of 172.17.10.5
packets with destination of 172.17.6.15	Serial0/0/0 ✓ packets with destination of 172.17.8.20
	The packet is dropped.

Explanation:

Packets with a destination of 172.17.6.15 are forwarded through Fa0/0. Packets with a destination of 172.17.12.10 are forwarded through Fa1/0. Packets with a destination of 172.17.14.8 are forwarded through Fa1/1. Because network 172.17.8.0 has no entry in the routing table, it will take the gateway of last resort, which means packets with destination 172.17.8.20 are forwarded through Serial0/0/0. Because a gateway of last resort exists, no packets will be dropped.

55. A medium-sized business is researching available options for connecting to the Internet. The company is looking for a high speed option with dedicated, symmetric access. Which connection type should the company choose?

- DSL
- dialup
- satellite
- leased line
- cable modem

56. What is the purpose of having a converged network?

- to provide high speed connectivity to all end devices
- to make sure that all types of data packets will be treated equally
- to achieve fault tolerance and high availability of data network infrastructure devices
- to reduce the cost of deploying and maintaining the communication infrastructure

Explanation:

With the development of technology, companies can now consolidate disparate networks onto one platform. A converged network, voice, video, and data travel over the same network, thus eliminating the need to create separate networks. This also reduces the costs associated with providing and maintaining the communication network infrastructure.

57. What characteristic of a network enables it to quickly grow to support new users and applications without impacting the performance of the service being delivered to existing users?

- reliability
- scalability
- quality of service
- accessibility

Explanation:

Networks must be able to quickly grow to support new users and services, without impacting existing users. This characteristic is known as scalability.

58. After several configuration changes are made to a router, the copy running-configuration startup-configuration command is issued. Where will the changes be stored?

- flash
- ROM
- NVRAM
- RAM
- the configuration register
- a TFTP server

59. Refer to the exhibit. From global configuration mode, an administrator is attempting to create a message-of-the-day banner by using the command banner motd V Authorized access only! Violators will be prosecuted! V When users log in using Telnet, the banner does not appear correctly. What is the problem?

```
Authorized access only!  
  
Router>
```

ITN Final Exam Form B Answers 001

- The banner message is too long.
- **The delimiting character appears in the banner message.**
- The symbol “!” signals the end of a banner message.
- Message-of-the-day banners will only appear when a user logs in through the console port.

60. What are three characteristics of an SVI? (Choose three.)

- It is designed as a security protocol to protect switch ports.
- **It is not associated with any physical interface on a switch.**
- It is a special interface that allows connectivity by different types of media.
- It is required to allow connectivity by any device at any location.
- **It provides a means to remotely manage a switch.**
- **It is associated with VLAN1 by default.**

Explanation:

Switches have one or more switch virtual interfaces (SVIs). SVIs are created in software since there is no physical interface for them. Virtual interfaces provide a means to remotely manage a switch over a network that is using IP. Each SVI is associated with a VLAN appearing in the default configuration “out-of-the-box.” The default SVI interface is VLAN1.

61. A technician configures a switch with these commands:

```
SwitchA(config)# interface vlan 1  
SwitchA(config-if)# ip address 192.168.1.1 255.255.255.0  
SwitchA(config-if)# no shutdown
```

What is the technician configuring?

- Telnet access
- **SVI**
- password encryption
- physical switchport access

Explanation:

For a switch to have an IP address, a switch virtual interface must be configured. This allows the switch to communicate with other devices on the network.

62. In computer communication, what is the purpose of message encoding?

- **to convert information to the appropriate form for transmission**
- to interpret information
- to break large messages into smaller frames

- to negotiate correct timing for successful communication

Explanation:

Before a message is sent across a network it must first be encoded. Encoding is the process of converting suitable for transmission across the physical medium. Each bit of the message is encoded into a pattern of impulses depending on the network media over which the bits are transmitted. The destination host receives the message and interprets the message.

63. What is the process of dividing a data stream into smaller pieces before transmission?

- segmentation
- encapsulation
- encoding
- flow control

Explanation:

Data streams would cause significant network congestion if they were transmitted as a single large stream. Data streams are segmented into smaller more manageable pieces which are then transmitted over the network.

64. When IPv4 addressing is manually configured on a web server, which property of the IPv4 configuration identifies the network and host portion for an IPv4 address?

- DNS server address
- subnet mask
- default gateway
- DHCP server address

Explanation:

There are several components that need to be entered when configuring IPv4 for an end device:

- **IPv4 address** – uniquely identifies an end device on the network
 - **Subnet mask** – determines the network address portion and host portion for an IPv4 address
 - **Default gateway** – the IP address of the router interface used for communicating with hosts in another network
 - **DNS server address** – the IP address of the Domain Name System (DNS) server
- DHCP server address (if DHCP is used) is not configured manually on end devices. It will be provided by the DHCP server when the device requests an IP address.

65. A network engineer is measuring the transfer of bits across the company backbone for a mission critical database application. The engineer notices that the network throughput appears lower than the bandwidth expected. Which three factors could influence the differences in throughput? (Choose three.)

- the amount of traffic that is currently crossing the network
- the sophistication of the encapsulation method applied to the data
- the type of traffic that is crossing the network
- the latency that is created by the number of network devices that the data is crossing
- the bandwidth of the WAN connection to the Internet
- the reliability of the gigabit Ethernet infrastructure of the backbone

Explanation:

Throughput usually does not match the specified bandwidth of physical links due to multiple factors. The traffic, type of traffic, and latency created by the network devices the data has to cross.

66. Which type of UTP cable is used to connect a PC to a switch port?

- console
- rollover
- crossover
- **straight-through**

Explanation:

A rollover cable is a Cisco proprietary cable used to connect to a router or switch console port. A straight-through cable is usually used to interconnect a host to a switch and a switch to a router. A crossover cable is used to interconnect, for example, between two switches, two routers, and two hosts.

67. What are two actions performed by a Cisco switch? (Choose two.)

- building a routing table that is based on the first IP address in the frame header
- **using the source MAC addresses of frames to build and maintain a MAC address table**
- forwarding frames with unknown destination IP addresses to the default gateway
- **utilizing the MAC address table to forward frames via the destination MAC address**
- examining the destination MAC address to add new entries to the MAC address table

Explanation:

Important actions that a switch performs are as follows:

- When a frame comes in, the switch examines the Layer 2 source address to build and maintain the Layer 2 MAC address table.
- It examines the Layer 2 destination address to determine how to forward the frame. When the destination address is known, the frame is sent out a particular port. When the address is unknown, the frame is sent to all ports in that network.

68. What are two examples of the cut-through switching method? (Choose two.)

- store-and-forward switching
- **fast-forward switching**
- CRC switching
- **fragment-free switching**
- QOS switching

Explanation:

Store-and forward switching accepts the entire frame and performs error checking using CRC before forwarding. Error checking is often required for QOS analysis. Fast-forward and fragment-free are both variations of the cut-through switching method. In fast-forward, the frame is received before the switch begins to forward it.

69. What information is added during encapsulation at OSI Layer 3?

- source and destination MAC

- source and destination application protocol
- source and destination port number
- **source and destination IP address**

Explanation:

IP is a Layer 3 protocol. Layer 3 devices can open the Layer 3 header to inspect the Layer 3 header which including the source and destination IP addresses.

70. Refer to the exhibit. The network administrator for a small advertising company has chosen to use the 192.168.5.96/27 network for internal LAN addressing. As shown in the exhibit, a static IP address is assigned to the company web server. However, the web server cannot access the Internet. The administrator verifies that local workstations with IP addresses that are assigned by a DHCP server can access the Internet, and the web server is able to ping local workstations. Which component is incorrectly configured?

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 5 . 98

Subnet mask: 255 . 255 . 255 . 224

Default gateway: 192 . 168 . 5 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 128 . 208 . 3 . 254

Alternate DNS server: . . .

ITN Final Exam Form B Answers 006

- subnet mask
- DNS address
- host IP address
- **default gateway address**

Explanation:

When a 255.255.255.224 subnet mask is used, the first three bits of the last octet are part of the network portion of the address. For the 192.168.5.96/27 network, valid host addresses are 192.168.5.97 through 192.168.5.126. The default gateway must be a Layer 3 device on the same network and it must contain an IP address within the valid IP address range.

71. Why does a Layer 3 device perform the ANDing process on a destination IP address and subnet mask?

- to identify the broadcast address of the destination network
- to identify the host address of the destination host
- to identify faulty frames
- to identify the network address of the destination network

Explanation:

ANDing allows us to identify the network address from the IP address and the network mask.

72. Which three addresses are valid public addresses? (Choose three.)

- 198.133.219.17
- 192.168.1.245
- 10.15.250.5
- 128.107.12.117
- 192.15.301.240
- 64.104.78.227

73. What type of IPv6 address is FE80::1?

- loopback
- link-local
- multicast
- global unicast

Explanation:

Link-local IPv6 addresses start with FE80::/10, which is any address from FE80:: to FEBF::. Link-local addresses allow directly connected devices to communicate with each other on the link they share.

74. Refer to the exhibit. On the basis of the output, which two statements about network connectivity are correct? (Choose two.)

```
C:\Windows\system32> tracert 192.168.100.1
Tracing route to 192.168.100.1 over a maximum of 30 hops
  0  1 ms    <1 ms   <1 ms   10.10.10.10
  1  2 ms    2 ms    1 ms    192.168.1.22
  2  2 ms    2 ms    1 ms    192.168.1.62
  3  2 ms    2 ms    1 ms    172.16.1.1
  4  2 ms    2 ms    1 ms    192.168.100.1
Trace complete.
```

ITN Final Exam Form B Answers 007

- There is connectivity between this device and the device at 192.168.100.1.
- The connectivity between these two hosts allows for videoconferencing calls.
- There are 4 hops between this device and the device at 192.168.100.1.
- The average transmission time between the two hosts is 2 milliseconds.
- This host does not have a default gateway configured.

Explanation:

The output displays a successful Layer 3 connection between a host computer and a host at 19.168.100.1. exist between them and the average transmission time is 1 milliseconds. Layer 3 connectivity does not ne can run between the hosts.

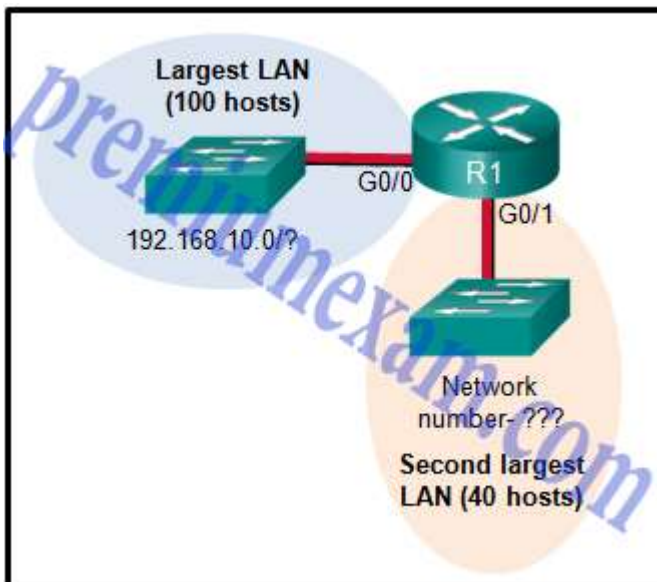
75. How many hosts are addressable on a network that has a mask of 255.255.255.248?

- 2
- 6
- 8
- 14
- 16
- 254

Explanation:

The subnet mask of 255.255.255.248 is the same as /29. This means the network portion of the address is 3 bits remain for host bits. $2^3 = 8$, but one of these addresses has to be used for the network number and broadcast address to reach all of the hosts on this network. That leaves only 6 usable IP addresses that can Don't forget that the default gateway must be one of these devices if this network is to communicate with

76. Refer to the exhibit. Consider the IP address of 192.168.10.0/24 that has been assigned to a high school building. The largest network in this building has 100 devices. If 192.168.10.0 is the network number for the largest network, what would be the network number for the next largest network, which has 40 devices?



ITN Final Exam Form B Answers 004

- 192.168.10.0
- 192.168.10.128

- 192.168.10.192
- 192.168.10.224
- 192.168.10.240

Explanation:

The first thing to calculate is what IP addresses are used by the largest LAN. Because the LAN has 100 hosts, the subnet mask must be 255.255.255.128. This would be a subnet mask of 255.255.255.128 for the largest LAN (192.168.10.0/25). The IP addresses 192.168.10.127, 192.168.10.0 is the network number (all 0s in the host bits) and 192.168.10.127 is the broadcast address (all 1s in the host bits). The next available IP address is the next network number – 192.168.10.128.

77. In what two situations would UDP be the preferred transport protocol over TCP? (Choose two.)

- when applications need to guarantee that a packet arrives intact, in sequence, and unduplicated
- **when a faster delivery mechanism is needed**
- when delivery overhead is not an issue
- **when applications do not need to guarantee delivery of the data**
- when destination port numbers are dynamic

Explanation:

UDP is a stateless protocol, which means that neither device on either end of the conversation must keep state. As a stateless protocol, UDP is used as the Layer 4 protocol for applications that need speedy (best-effort) delivery of data, such as the transport of digitized voice or video.

78. What important information is added to the TCP/IP transport layer header to ensure communication and connectivity with a remote network device?

- timing and synchronization
- **destination and source port numbers**
- destination and source physical addresses
- destination and source logical network addresses

Explanation:

The destination and source port numbers are used to identify exactly which protocol and process is requested.

79. What is the TCP mechanism used in congestion avoidance?

- three-way handshake
- socket pair
- two-way handshake
- **sliding window**

Explanation:

TCP uses windows to attempt to manage the rate of transmission to the maximum flow that the network can handle while minimizing loss and retransmissions. When overwhelmed with data, the destination can send a request for the sender to slow down. This congestion avoidance is called sliding windows.

80. Which three statements characterize UDP? (Choose three.)

- UDP provides basic connectionless transport layer functions.
- UDP provides connection-oriented, fast transport of data at Layer 3.
- UDP relies on application layer protocols for error detection.
- UDP is a low overhead protocol that does not provide sequencing or flow control mechanisms.
- UDP relies on IP for error detection and recovery.
- UDP provides sophisticated flow control mechanisms.

Explanation:

UDP is a simple protocol that provides the basic transport layer functions. It has much lower overhead than TCP, is connection-oriented and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that TCP does.

81. Which two protocols operate at the highest layer of the TCP/IP protocol stack? (Choose two.)

- DNS
- Ethernet
- IP
- POP
- TCP
- UDP

Explanation:

The application layer is the top layer of the TCP/IP protocol stack. Application layer protocols include HTTP, SMTP, IMAP, FTP, and POP.

82. Which two roles can a computer assume in a peer-to-peer network where a file is being shared between two computers? (Choose two.)

- client
- master
- server
- slave
- transient

Explanation:

In a peer-to-peer (P2P) network, two or more computers are connected and can share resources without the need for a central server. In this type of network, one computer that has the file acts as a server for the device (the client) that requests the file.

83. What is the function of the HTTP GET message?

- to request an HTML page from a web server
- to send error information from a web server to a web client
- to upload content to a web server from a web client
- to retrieve client email from an email server using TCP port 110

Explanation:

There are three common HTTP message types:

1. GET – used by clients to request data from the web server
2. POST – used by clients to upload data to a web server

3. PUT – used by clients to upload data to a web server

84. When planning for network growth, where in the network should packet captures take place to assess network traffic?

- on as many different network segments as possible
- only at the edge of the network
- between hosts and the default gateway
- only on the busiest network segment

Explanation:

Because some types of traffic will be only on specific network segments, packet captures for analysis should be taken on as many segments as possible.

85. Refer to the exhibit. An administrator is testing connectivity to a remote device with the IP address 10.1.1.1. What does the output of this command indicate?

```
Switch# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

ITN Final Exam Form B Answers 002

- Connectivity to the remote device was successful.
- A router along the path did not have a route to the destination.
- A ping packet is being blocked by a security device along the path.
- The connection timed out while waiting for a reply from the remote device.

Explanation:

In the output of the ping command, an exclamation mark (!) indicates a response was successfully received, a period (.) indicates the connection timed out while waiting for a reply, and the letter “U” indicates that a router along the path did not have a route to the destination and sent an ICMP destination unreachable message back to the source.

86. A user is unable to reach the web site when typing <http://www.cisco.com> in a web browser, but can reach the same site by typing <http://72.163.4.161>. What is the issue?

- default gateway
- DHCP
- DNS
- TCP/IP protocol stack

Explanation:

Domain Name Service (DNS) is used to translate a web address to an IP address. The address of the DNS server is configured on the client computers.

87. What source IP address does a router use by default when the traceroute command is issued?

- the highest configured IP address on the router
- a loopback IP address
- the IP address of the outbound interface
- the lowest configured IP address on the router

Explanation:

When sending an echo request message, a router will use the IP address of the exit interface as the source. This can be changed by using an extended ping and specifying a specific source IP address.

88. Match each item to the type of topology diagram on which it is typically identified. (Not all options are used.)

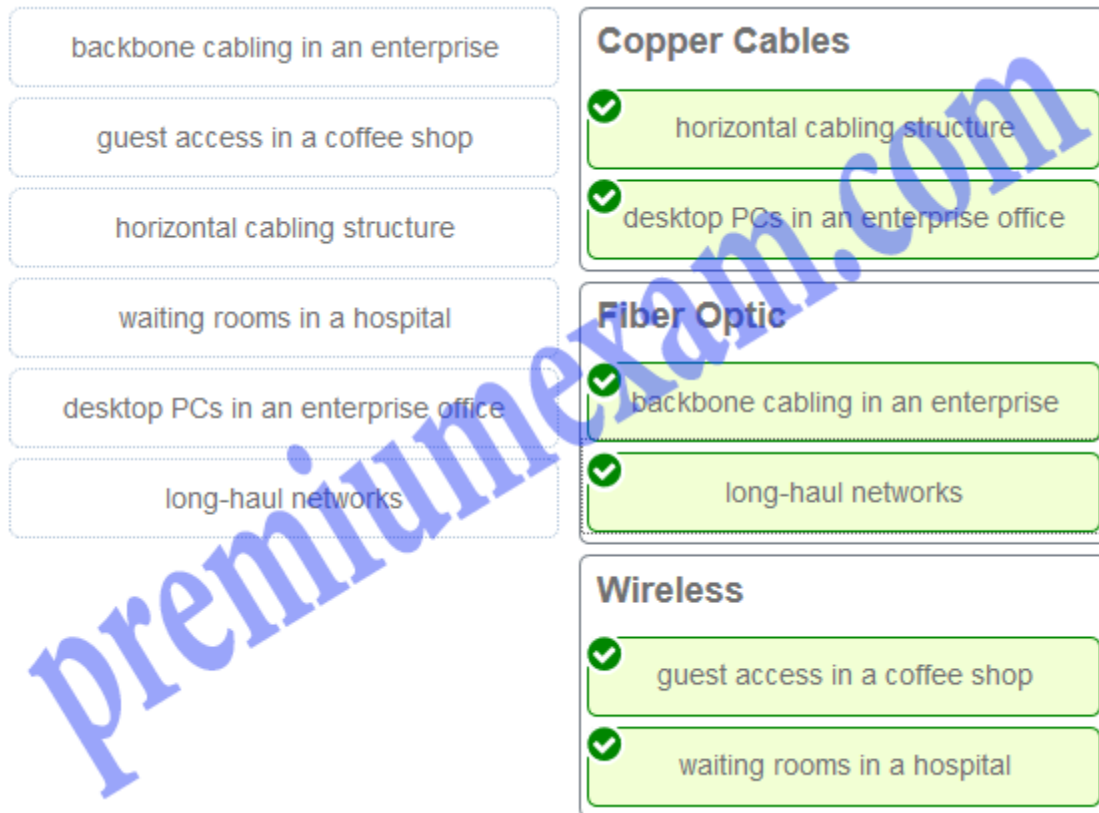
IP address of a server	physical topology diagram ☒ location of a desktop PC in a classroom ☒ path of cables that connect rooms to wiring closets
location of a desktop PC in a classroom	
USB port on a desktop PC in a classroom	
path of cables that connect rooms to wiring closets	logical topology diagram ☒ IP address of a server

ITN Final Exam Form B Answers 01

Explanation:

A logical topology diagram typically depicts the IP addressing scheme and groupings of devices and ports. A physical topology diagram typically depicts how those devices are connected to each other and the network, focusing on the physical locations of intermediate devices and the physical locations of intermediate cabling.

89. Match the situation with the appropriate use of network media.



ITN Final Exam Form B Answers 03

Explanation:

Copper Cables – horizontal cabling structure and desktop PCs in offices in an enterprise

Fiber optic – backbone cabling in an enterprise and long-haul networks

Wireless – coffee shops and waiting rooms in a hospital

90. A company is expanding its business to other countries. All branch offices must remain connected to corporate headquarters at all times. Which network technology is required to support this requirement?

- LAN
- MAN
- **WAN**
- WLAN

Explanation:

A local-area network (LAN) normally connects end users and network resources over a limited geographic area. A wireless LAN (WLAN) serves the same purpose as a LAN but uses wireless technologies. A metropolitan-area network (MAN) connects networks together over a large geographic area such as a city, and a wide-area network (WAN) connects networks together over a large geographic area, such as cities, countries, or the globe.

91. A home user is looking for an ISP connection that provides high speed digital transmission over regular phone lines. What ISP connection type should be used?

- DSL
- dial-up
- satellite
- cell modem
- cable modem

92. How does quality of service help a network support a wide range of applications and services?

- by limiting the impact of a network failure
- by allowing quick recovery from network failures
- by providing mechanisms to manage congested network traffic
- by providing the ability for the network to grow to accommodate new users

Explanation:

Quality of service (QoS), is a vital component of the architecture of a network. With QoS, network administrators can provide predictable and measurable service guarantees through mechanisms that manage congested network traffic.

93. After making configuration changes on a Cisco switch, a network administrator issues a copy running-config startup-config command. What is the result of issuing this command?

- The new configuration will be stored in flash memory.
- The new configuration will be loaded if the switch is restarted.
- The current IOS file will be replaced with the newly configured file.
- The configuration changes will be removed and the original configuration will be restored.

Explanation:

With the **copy running-config startup-config** command, the content of the current operating configuration is saved to the startup configuration file stored in NVRAM. The configuration file saved in NVRAM will be loaded when the device is restarted.

94. Refer to the exhibit. A network administrator is configuring access control to switch SW1. If the administrator has already logged into a Telnet session on the switch, which password is needed to access privileged EXEC mode?

```

Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# enable password letmein
SW1(config)# enable secret secretin
SW1(config)# line console 0
SW1(config-line)# password lineconin
SW1(config-line)# login
SW1(config-line)# exit
SW1(config)# line vty 0 15
SW1(config-line)# password linevtyin
SW1(config-line)# login
SW1(config-line)# end
SW1#

```

ITN Final Exam Form C Answers 001

- letmein
- **secretin**
- lineconin
- linevtyin

Explanation:

Telnet accesses a network device through the virtual interface configured with the **line VTY** command. The password configured under the **line console 0** command is required to access the user EXEC mode. The password configured under the **line vty 0 15** command is required to access the privileged EXEC mode. The enable and enable secret passwords are used to allow entry into the privileged EXEC mode.

95. What function does pressing the Tab key have when entering a command in IOS?

- It aborts the current command and returns to configuration mode.
- It exits configuration mode and returns to user EXEC mode.
- It moves the cursor to the beginning of the next line.
- **It completes the remainder of a partially typed word in a command.**

Explanation:

Pressing the Tab key after a command has been partially typed will cause the IOS to complete the rest of the command.

96. What is a characteristic of multicast messages?

- **They are sent to a select group of hosts.**
- They are sent to all hosts on a network.
- They must be acknowledged.
- They are sent to a single destination.

Explanation:

Multicast is a one-to-many type of communication. Multicast messages are addressed to a specific multicast group.

97. What layer is responsible for routing messages through an internetwork in the TCP/IP model?

- **internet**
- transport
- network access

- session

Explanation:

The TCP/IP model consists of four layers: application, transport, internet, and network access. Of these four, the network access layer is responsible for routing messages. The session layer is not part of the TCP/IP model but is rather part of the OSI model.

98. Which statement accurately describes a TCP/IP encapsulation process when a PC is sending data to the network?

- Data is sent from the internet layer to the network access layer.
- Packets are sent from the network access layer to the transport layer.
- **Segments are sent from the transport layer to the internet layer.**
- Frames are sent from the network access layer to the internet layer.

Explanation:

When the data is traveling from the PC to the network, the transport layer sends segments to the internet layer, which creates packets to the network access layer, which creates frames and then converts the frames to bits. The bits are then sent to the network access layer.

99. What unique address is embedded in an Ethernet NIC and used for communication on an Ethernet network?

- host address
- IP address
- **MAC address**
- network address

Explanation:

The MAC address is a 48-bit address that is burned into every Ethernet NIC. Each MAC address is unique to the NIC.

100. Which procedure is used to reduce the effect of crosstalk in copper cables?

- requiring proper grounding connections
- **twisting opposing circuit wire pairs together**
- wrapping the bundle of wires with metallic shielding
- designing a cable infrastructure to avoid crosstalk interference
- avoiding sharp bends during installation

Explanation:

In copper cables, crosstalk is a disturbance caused by the electric or magnetic fields of a signal on one wire interfering with the signal on an adjacent wire. Twisting opposing circuit wire pairs together can effectively cancel the crosstalk. The other two options counter the negative effects of EMI and RFI, but not crosstalk.

101. During the encapsulation process, what occurs at the data link layer for a PC connected to an Ethernet network?

- An IP address is added.
- The logical address is added.
- **The physical address is added.**
- The process port number is added.

Explanation:

The Ethernet frame includes the source and destination physical address. The trailer includes a CRC value to allow the receiving device to determine if the frame has been changed (has errors) during the transmission.

**102. What are two characteristics of Ethernet MAC addresses?
(Choose two.)**

- They are globally unique.
- They are routable on the Internet.
- They are expressed as 12 hexadecimal digits.
- MAC addresses use a flexible hierarchical structure.
- MAC addresses must be unique for both Ethernet and serial interfaces on a device.

Explanation:

An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits. MAC addresses must be unique. MAC addresses are in flat structure and thus they are not routable on the Internet. Serial interfaces do not have MAC addresses.

103. If a device receives an Ethernet frame of 60 bytes, what will it do?

- drop the frame
- process the frame as it is
- send an error message to the sending device
- add random data bytes to make it 64 bytes long and then forward it

Explanation:

Ethernet standards define the minimum frame size as 64 bytes. A frame less than 64 bytes is considered a runt frame and is automatically discarded by receiving devices.

**104. Under which two circumstances will a switch flood a frame out of every port except the port that the frame was received on?
(Choose two.)**

- The frame has the broadcast address as the destination address.
- The destination address is unknown to the switch.
- The source address in the frame header is the broadcast address.
- The source address in the frame is a multicast address.
- The destination address in the frame is a known unicast address.

Explanation:

A switch will flood a frame out of every port, except the one that the frame was received from, under two circumstances: if the destination address is the broadcast address, or the destination address is unknown to the switch.

105. Which switching method has the lowest level of latency?

- cut-through
- store-and-forward
- fragment-free
- fast-forward

Explanation:

Fast-forward switching begins to forward a frame after reading the destination MAC address, resulting in reads the first 64 bytes before forwarding. Store-and-forward has the highest latency because it reads the entire frame before forwarding it. Both fragment-free and fast-forward are types of cut-through switching.

106. Which two commands can be used on a Windows host to display the routing table? (Choose two.)

- netstat -s
- **route print**
- show ip route
- **netstat -r**
- tracert

Explanation:

On a Windows host, the **route print** or **netstat -r** commands can be used to display the host routing table output. On a router, the **show ip route** command is used to display the routing table. The **netstat -s** command displays statistics. The **tracert** command is used to display the path that a packet travels to its destination.

107. Which two functions are primary functions of a router? (Choose two.)

- **packet forwarding**
- microsegmentation
- domain name resolution
- **path selection**
- flow control

108. What is the binary representation of 0xCA?

- 10111010
- 11010101
- **11001010**
- 11011010

Explanation:

When converted, CA in hex is equivalent to 11011010 in binary. One way to do the conversion is one nibble at a time. CA is 1101 and 1010. Combine the two nibbles gives 11011010.

109. At a minimum, which address is required on IPv6-enabled interfaces?

- **link-local**
- unique local
- site local
- global unicast

Explanation:

All IPv6 enabled interfaces must at minimum have a link-local address. Other IPv6 addresses can be assigned to the interface.

110. Which service provides dynamic global IPv6 addressing to end devices without using a server that keeps a record of available IPv6 addresses?

- stateful DHCPv6
- **SLAAC**
- static IPv6 addressing
- stateless DHCPv6

Explanation:

Using stateless address autoconfiguration (SLAAC), a PC can solicit a router and receive the prefix length information the PC can then create its own IPv6 global unicast address.

111. What is the purpose of the command ping ::1?

- **It tests the internal configuration of an IPv6 host.**
- It tests the broadcast capability of all hosts on the subnet.
- It tests the multicast connectivity to all hosts on the subnet.
- It tests the reachability of the default gateway for the network.

Explanation:

The address ::1 is an IPv6 loopback address. Using the command **ping ::1** tests the internal IP stack to ensure it is functioning correctly. It does not test reachability to any external device, nor does it confirm that IPv6 addresses are configured on the host.

112. How many usable IP addresses are available on the 192.168.1.0/27 network?

- 256
- 254
- 62
- **30**
- 16
- 32

Explanation:

A /27 mask is the same as 255.255.255.224. This leaves 5 host bits. With 5 host bits, 32 IP addresses are available on the subnet number and one address represents the broadcast address. Thus, 30 addresses can then be used for hosts.

113. A network administrator wants to have the same subnet mask for three subnetworks at a small site. The site has the following networks and numbers of devices:

Subnetwork A: IP phones – 10 addresses

Subnetwork B: PCs – 8 addresses

Subnetwork C: Printers – 2 addresses

What single subnet mask would be appropriate to use for the three subnetworks?

- 255.255.255.0
- **255.255.255.240**
- 255.255.255.248
- 255.255.255.252

Explanation:

If the same mask is to be used, then the network with the most hosts must be examined for number of host bits are needed. The /28 or 255.255.255.240 subnet mask would be appropriate to use for these networks.

114. What subnet mask is needed if an IPv4 network has 40 devices that need IP addresses and address space is not to be wasted?

- 255.255.255.0
- 255.255.255.128
- 255.255.255.192
- 255.255.255.224
- 255.255.255.240

Explanation:

In order to accommodate 40 devices, 6 host bits are needed. With 6 bits, 64 addresses are possible, but one address is for a broadcast. This leaves 62 addresses that can be assigned to network devices. The subnet mask for addressing is 255.255.255.192.

115. What are two characteristics shared by TCP and UDP? (Choose two.)

- default window size
- connectionless communication
- port numbering
- 3-way handshake
- ability to carry digitized voice
- use of checksum

Explanation:

Both TCP and UDP use source and destination port numbers to distinguish different data streams and to forward data to the right applications. Error checking the header and data is done by both protocols by using a checksum calculation on the data that is received. TCP is connection-oriented and uses a 3-way handshake to establish an initial connection and regulate the amount of traffic sent before receiving an acknowledgment. UDP is connectionless and is the preferred protocol for VoIP signals.

116. Why are port numbers included in the TCP header of a segment?

- to indicate the correct router interface that should be used to forward a segment
- to identify which switch ports should receive or forward the segment
- to determine which Layer 3 protocol should be used to encapsulate the data
- to enable a receiving host to forward the data to the appropriate application
- to allow the receiving host to assemble the packet in the proper order

117. What is an example of a top-level domain?

- www.cisco.com
- cisco.com
- .com
- root.cisco.com

Explanation:

Top-level domains represent a country or type of organization, such as .com or .edu.

118. What is one difference between the client-server and peer-to-peer network models?

- Only in the client-server model can file transfers occur.
- **Every device in a peer-to-peer network can function as a client or a server.**
- A peer-to-peer network transfers data faster than a transfer using a client-server network.
- A data transfer that uses a device serving in a client role requires that a dedicated server be present.

Explanation:

Data transfer speeds depend on a number of factors including the amount of traffic, the quality of service. Transfer speeds are not dependent on the network model type. File transfers can occur using the client-server model. A data transfer between a device acting in the client role and a device acting in the server role can occur in peer-to-peer networks.

119. Which networking model is being used when an author uploads one chapter document to a file server of a book publisher?

- peer-to-peer
- master-slave
- **client/server**
- point-to-point

Explanation:

In the client/server network model, a network device assumes the role of server in order to provide a partial storage. In the client/server network model, a dedicated server does not have to be used, but if one is present, it is the client/server model. In contrast, a peer-to-peer network does not have a dedicated server.

120. What network service resolves the URL entered on a PC to the IP address of the destination server?

- **DNS**
- DHCP
- FTP
- SNMP

Explanation:

When a client attempts to connect to a website, the destination URL must be resolved to an IP address. This is done by the Domain Name System (DNS) server.

121. A network engineer is analyzing reports from a recently performed network baseline. Which situation would depict a possible latency issue?

- a change in the bandwidth according to the show interfaces output
- a next-hop timeout from a traceroute
- **an increase in host-to-host ping response times**
- a change in the amount of RAM according to the show version output

Explanation:

While analyzing historical reports an administrator can compare host-to-host timers from the **ping** command to identify network issues.

122. Which firewall feature is used to ensure that packets coming into a network are legitimate responses to requests initiated from internal hosts?

- **stateful packet inspection**
- URL filtering
- application filtering
- packet filtering

Explanation:

Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests initiated from inside the network. Packet filtering can be used to permit or deny access to resources based on IP or MAC address. Application filtering can permit or deny access based on port number. URL filtering is used to permit or deny access based on URL.

123. What is one indication that a Windows computer did not receive an IPv4 address from a DHCP server?

- The computer cannot ping 127.0.0.1.
- Windows displays a DHCP timeout message.
- **The computer receives an IP address that starts with 169.254.**
- The computer cannot ping other devices on the same network with IP addresses in the 169.254.0.0/16 range.

Explanation:

When a Windows PC cannot communicate with an IPv4 DHCP server, the computer automatically assigns an IP address from the 169.254.0.0/16 range. Any other device on the same network that receives an address in the same range is reachable.

124. Which command can an administrator issue on a Cisco router to send debug messages to the vty lines?

- **terminal monitor**
- logging console
- logging buffered
- logging synchronous

Explanation:

Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the vty lines is done with the **terminal monitor** command.